UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/741,510	12/19/2003	Guruprashanth A. Bellipady	33692.03.3632	4449

23418 7590 03/15/2007
VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/741,510	BELLIPADY ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Presently, pending claims are 1 – 24.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, 10, 18 and 22, Applicant asserts that (a) Zubeldia does not teach certificate revocation notifications that are transmitted over a broadcast channel (and used in a mobile device) (Remarks: Page 9 Line 6 – 8), (b) Zubeldia does not teach a certification identifier or signed comparison data (Remarks: Page 8, Last sentence) and (c) no motivation to combine the teaching of Simon with Zubeldia (Remarks: Page 8, 2nd Para, Line 3 – 4). Examiner respectfully disagrees with the following reasons:

- Regarding argument (a), Examiner notes, according to MPEP § 2145, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Examiner asserts Simon is relied upon providing certificate revocation notifications that are transmitted over a broadcast channel (and used in a mobile device) (Simon: Para [0076] and Par [0110] – [0111]: certificate exclusion / revocation notification message is broadcasted over the mesh network implemented in a wireless system environment including mobile appliance) and Zubeldia is relied upon providing a more detail context description about each entry of certificate exclusion / revocation notification on a CRL

(Certificate Revocation List) (Zubeldia: Column 3 Line 10 – 14 and Column 4 Line 8 – 40).

- Regarding argument (b), Examiner notes Zubeldia does teach a certification identifier (Zubeldia: Column 4 Line 14: certificate serial number is qualified as a certificate identifier) or signed comparison data (Zubeldia: Column 2 Line 50 – 54 and Column 4 Line 8 – 18 / Line 4 – 7: (a) a digital signature data used is qualified as a signed comparison data (b) Zubeldia teaches providing the report format of an certificate revocation notification presented as an entry on a CRL (Certificate Revocation List) and each entry is corresponding to a particular certificate of interests).

- Regarding argument (c), Applicant argues Examiner has not provided a motivation to combine the references. Examiner disagrees. Sufficient motivation is provided to combine the references – Please see the reasons as that set forth in the following Office action that is repeated herein. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Zubeldia within the system of Simon because (a) Simon teaches providing the control and accountability through the use of digital certificate and associated revocation notification over a wireless network environment – for example, when an end device is compromised, the suspected end device certificate is excluded / revoked and broadcasted over the wireless network (Simon: Para [0004], [0076] an Para [0110] – [0111]), and (b) Zubeldia teaches providing a more detail context description about each entry of certificate exclusion / revocation notification on a CRL (Certificate Revocation List) and the report format of an revocation notification presented as an entry on a CRL

where each entry is corresponding to a particular certificate of interests (Zubeldia: Column 3 Line 10 – 14 and Column 4 Line 8 – 40 and Column 4 Line 4 – 40).

4. Furthermore, Applicant asserts the prior-arts fails to teach "generating a first verification value from the signed comparison data and the data representing a certificate of interest and generating a second verification value based on the certification authority identifier and the revocation reason data (Remarks: Page 10 Line 5 – 9). Examiner disagrees because Zubeldia teaches (a) providing notifications of certificate revocations including a list of digital certificates (Zubeldia: Column 3 Line 9 – 12) and (b) providing a signature to authenticate the respective certificate by computing a message digest (Zubeldia: Column 2 Line 48 – 54: i.e. a verification value) for verification purpose and (c) the certificate entry values include the certification authority identifier (Zubeldia: Column 4 Line 5 – 6 & Figure 7 / Element 720) and the revocation reason data (Zubeldia: Column 8 Line 7 – 8 & Figure 7 / Element 765) and as such a first verification value and a second verification value, as recited in the claim, can then be computed, compared and authenticated accordingly by one of the ordinary skill in the art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 – 6, 9 – 15, 18, 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (U.S. Patent 2005/0135268), in view of Zubeldia et al. (U.S. Patent 6044462).

As per claim 22 (and claim 1, 10 & 18), Simon teaches a method for providing certificate based cryptography in a mobile device, the method comprising:

receiving a certificate revocation notification from a wireless transmission over a broadcast channel (Simon: Para [0004], [0076] an Para [0110] – [0111]: providing the control and accountability through the use of digital certificate and associated revocation notification over a wireless network environment – for example, when an end device is compromised, the suspected end device certificate is excluded / revoked and broadcasted over the wireless network). However, Simon does not disclose expressly about the context details of the certificate revocation notification.

Zubeldia teaches wherein the certificate revocation notification includes a certification authority identifier, revocation reason data, signed comparison data and data representing a certificate of interest (Zubeldia: Figure 2, Column 4 Line 1 – 20,

Column 3 Line 10 – 20, Column 1 Line 20 – 42 and Column 2 Line 22 – the certification authority identifier (Column 4 Line 5 – 6 & Figure 7 / Element 720) and the revocation reason data (Column 8 Line 7 – 8 & Figure 7 / Element 765)).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Zubeldia within the system of Simon because (a) Simon teaches providing the control and accountability through the use of digital certificate and associated revocation notification over a wireless network environment – for example, when an end device is compromised, the suspected end device certificate is excluded / revoked and broadcasted over the wireless network (Simon: Para [0004], [0076] an Para [0110] – [0111]), and (b) Zubeldia teaches providing a more detail context description about each entry of certificate exclusion / revocation notification on a CRL (Certificate Revocation List) and the report format of an revocation notification presented as an entry on a CRL where each entry is corresponding to a particular certificate of interests (Zubeldia: Column 3 Line 10 – 14 and Column 4 Line 8 – 40 and Column 4 Line 4 – 40).

providing a method for effectively managing digital certificate revocation in a cryptographic environment (Zubeldia: Column 1 Line 5 – 8).

authenticating the certificate revocation notification (Zubeldia: Column 3 Line 9 – 12, Column 2 Line 48 – 49 and Column 1 Line 20 – 42), wherein the authenticating includes:

generating a first verification value from the signed comparison data and the data representing a certificate of interest; and generating a second verification value based

on the certification authority identifier and the revocation reason data (Zubeldia: Column 3 Line 10 – 20, Column 1 Line 20 – 42 and Column 2 Line 50 – 54: Zubeldia teaches (a) providing notifications of certificate revocations including a list of digital certificates (Zubeldia: Column 3 Line 9 – 12) and (b) providing a signature to authenticate the respective certificate by computing a message digest (Zubeldia: Column 2 Line 48 – 54: i.e. a verification value) for verification purpose and (c) the certificate entry values include the certification authority identifier (Column 4 Line 5 – 6 & Figure 7 / Element 720) and the revocation reason data (Column 8 Line 7 – 8 & Figure 7 / Element 765) and as such a first verification value and a second verification value, as recited in the claim, can then be computed, compared and authenticated accordingly by one of the ordinary skill in the art.); and

comparing the first verification value with the second verification value (Zubeldia: Column 3 Line 10 – 20, Column 1 Line 20 – 42 and Column 2 Line 50 – 54); and

updating data representing at least one private or public key based on the certificate revocation notification (Zubeldia: Column 3 Line 60 – 67).

As per claim 2, 11 and 19, Simon as modified teaches the certificate revocation notification includes a certification authority identifier, revocation reason data, and data representing a certificate of interest (Zubeldia: Figure 2, Column 4 Line 1 – 13).

As per claim 3, Simon as modified teaches a searcher operative to receive the certification authority identifier from the authentication module, the searcher operative to

retrieve a stored certificate corresponding to the certification authority identifier (Zubeldia: Column 3 Line 21 – 30, Column 3 Line 46 and Column 4 Line 5 – 7).

As per claim 4 and 12, Simon as modified teaches the authenticator further includes a first verification value generator operative to generate a first verification value based on the signed comparison data and the data representing a certificate of interest; a second verification value generator operative to generate a second verification value based on the certification authority identifier and the revocation reason data; and a comparator operative to compare to the first verification value and the second verification value (Zubeldia: Column 3 Line 10 – 20, Column 1 Line 20 – 42 and Column 2 Line 50 – 54).

As per claim 5, Simon as modified teaches the signed comparison data is a compressed representation of the combination of the certification authority identifier and the revocation reason data using a hash algorithm (Zubeldia: Column 1 Line 30: Hash (or MD) is indeed a compressed representation of a more complete data information).

As per claim 6 and 15, Simon as modified teaches the data representing a certificate of interest is at least one of: a certificate and a universal resource locator (Zubeldia: Column 3 Line 21 – 30, Column 3 Line 46 and Column 4 Line 5 – 7).

As per claim 9, Simon as modified teaches a user interface coupled to the searcher, the user interface operative to receive user display information regarding the

certificate revocation notification and the user interface coupled to the updater wherein the updater is operative to update the data representing at least one private or public key based on a user input received by the user interface module (Zubeldia: Column 5 Line 10 – 25 and Column 6 Line 15 – 23).

As per claim 13, Simon as modified teaches accessing data representing at least one private or public key Zubeldia: Column 2 Line 10 – 19); and retrieving a certificate based on the certification authority identifier (Zubeldia: Column 3 Line 21 – 30, Column 3 Line 46 and Column 4 Line 5 – 7).

6. Claims 7, 8, 16, 17, 20, 21 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (U.S. Patent 2005/0135268), in view of Zubeldia et al. (U.S. Patent 6044462), and in view of Kenagy et al. (U.S. Patent 2004/0110504).

As per claim 7, 16, 21 and 24, Simon as modified teaches receiving a certificate revocation notification from a wireless transmission over a broadcast channel (Simon: Para [0076] and [0067]). Simon as modified does not teach the channel is at least one of: a dedicated broadcast channel and a channel assigned a predetermined port identifier in a messaging system.

Kenagy teaches the channel is at least one of: a dedicated broadcast channel and a channel assigned a predetermined port identifier in a messaging system (Kenagy: Para [0023] Line 14 – 17).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kenagy within the system of Simon as modified because (a) Simon teaches providing the control and accountability through the use of digital certificate over a spontaneously-formed wireless network environment (Simon: Para [0004] & [0076]), and (b) Kenagy teaches a method for effective handshaking between the wireless device and server / router by using the SMS (Short Message Service) (Kenagy: Para [0023] Line 14 – 17).

As per claim 8 and 17 and 20, Simon as modified teaches the messaging system is at least one of a: short messaging system and an extended messaging system (Kenagy: Para [0023] Line 14 – 17) & (Simon: Para [0076] and [0067]).

7. Claims 14 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (U.S. Patent 2005/0135268), in view of Zubeldia et al. (U.S. Patent 6044462), and in view of Shrader et al. (U.S. Patent 6775771).

As per claim 14, Simon as modified teaches displaying friendly name data extracted from the certificate revocation notification and the revocation reason data (Zubeldia: Column 5 Line 10 – 25 and Column 6 Line 15 – 23 & Figure 1). However, Simon as modified does not disclose expressly querying an end user to remove the certificate from the data representing a certificate of interest.

Shrader teaches querying an end user to remove the certificate from the data representing a certificate of interest (Shrader: Column 14 Line 42 – 45).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shrader within the system of Simon as modified because (a) Simon teaches providing the control and accountability through the use of digital certificate over a spontaneously-formed wireless network environment (Simon: Para [0004] & [0076]), and (b) Shrader teaches an improved method for presenting and manipulating secure data objects within heterogeneous networks in a distributed computing environment (Shrader: Column 3 Line 33 – 37).

As per claim 23, claim 23 encompasses the similar scope as described in claim 13 and claim 14. Therefore, see same rationale addressed above in rejecting claim 13 and claim 14.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

LBC